NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION

Strategic Plan

Introduction

The NICE Strategic Plan is the result of engagement and deliberation among NICE partners in government, academia, and industry. The plan outlines a vision, mission, values, and goals and objectives for NICE. NICE partners will continue to develop appropriate implementation strategies and metrics.

Vision

A digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

Mission

To energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

Values

Seek Evidence – inform actions or decisions with data and pursue objective and reliable sources of information

Pursue Action – create concrete steps towards deliverable outcomes to achieve mission and goals

Challenge Assumptions – examine rationale for past and present education, training, and workforce approaches and apply critical analysis to future solutions

Embrace Change – seek creative and innovative solutions that might disrupt or defy the status quo

Stimulate Innovation – inspire and experiment with new approaches to education, training, and skills development

Foster Communication – raise awareness of cybersecurity education and workforce issues and encourage openness to build trust

Facilitate Collaboration – combine the knowledge and skills of multiple stakeholders with multiple viewpoints to achieve the best outcomes

Share Resources – leverage, support, and raise awareness of community-developed approaches and solutions

Model Inclusion – encourage participation from stakeholders with diverse backgrounds and viewpoints

Measure Results – assess the effectiveness of results through both quantitative metrics and qualitative measures

Goal 1

ACCELERATE LEARNING AND SKILLS DEVELOPMENT

Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers

OBJECTIVES

1.1 Stimulate the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers

1.2 Advance programs that reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles

1.3 Engage displaced workers or underemployed individuals who are available and motivated to assume cybersecurity work roles

1.4 Experiment with the use of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills

1.5 Promote efforts to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce needs

Goal 2

NURTURE A DIVERSE LEARNING COMMUNITY

Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

OBJECTIVES

2.1 Improve education programs, co-curricular experiences, and training and certifications

2.2 Promote tools and techniques that effectively measure and validate individual aptitude, knowledge, skills, and abilities

2.3 Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school

2.4 Expand creative and effective efforts to increase the number of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce

2.5 Support the development and dissemination of academic pathways for cybersecurity careers

Goal 3

GUIDE CAREER DEVELOPMENT AND WORKFORCE PLANNING

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

OBJECTIVES

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the National Cybersecurity Workforce Framework and encourage adoption

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

Overview of NICE Engagement Process

The NICE Interagency Coordinating Council and the NICE Working Group will establish plans and metrics to ensure successful implementation of the plan. Below is a brief description of each group.

NICE INTERAGENCY COORDINATING COUNCIL

The NICE Interagency Coordinating Council convenes federal government partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development. The meetings will provide an opportunity for the NICE Program Office located at NIST to communicate program updates with key partners in the federal government to learn about other federal government activities in support of NICE. The group will also identify and discuss policy issues and provide input into the strategic directions for NICE.

NICE WORKING GROUP

The NICE Working Group provides a mechanism for public and private sector participants to develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The meetings provide an opportunity for consultation and information-sharing between the government, academia, and the private sector. The NICE Working Group also identifies new initiatives that support the strategic objectives of NICE. To join the NICE Working Group monthly meetings and to be added to the NICE Working Group mailing list, please send an email to nicewg-request@nist.gov with your full name and email address in the body of the message.

About NICE Program Office at NIST

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure.

NICE Communication Channels

NICE WEBSITE

nist.gov/nice

NICE eNEWSLETTER

nist.gov/nice/enewsletter

NICE EMAIL DISTRIBUTION LIST

tinyurl.com/niceupdates

NICE WEBINAR SERIES

nist.gov/nice/webinars